

AMENDMENTS TO THE CLAIMS

There are no amendments to the Claims. The pending Claims are reproduced here for the convenience of the Examiner.

Claims 1 – 28 (canceled).

29. (Previously Presented) A method for assisting a user in verifying a cast ballot B_{cast} stored in a server, the method comprising:

forming a digital signature of B_{cast} using a private key of the server $DS(B_{\text{cast}}, s)$;
 associating the B_{cast} and $DS(B_{\text{cast}}, s)$ with a vote serial number VSN;
 forming a confirmation token, comprising $DS(B_{\text{cast}}, s)$ and VSN;
 making the confirmation token available to a user;
 receiving a confirmation token made available to a user;
 extracting $VSN_{\text{received token}}$ and $DS_{\text{received token}}(B_{\text{cast}}, s)$ from the received token; and
 for VSN equal to $VSN_{\text{received token}}$, comparing $DS_{\text{received token}}(B_{\text{cast}}, s)$ and at least one of
 $DS(B_{\text{cast}}, s)$ and $DS(B_{\text{cast}}, S)$;
 if the comparison shows equivalence between the data compared, determining that B_{cast} is
 verified.

30. (Previously Presented) The method of Claim 29 wherein:

the confirmation token further comprises a digital signature of an aggregation comprising
 the associated B_{cast} and VSN using the server's private key $DS(\text{Aggregation}, s)$,
 extracting $DS_{\text{received token}}(\text{Aggregation}, s)$ from the received token; and
 B_{cast} is verified only upon the additional condition that $DS_{\text{received token}}(\text{Aggregation}, s)$ is
 equivalent to $DS(\text{Aggregation}, s)$.

31. (Previously Presented) A method for assisting a user in verifying a cast ballot recorded in a server, the method comprising:

receiving in a server at least one set of:

a cast ballot B_{cast} and

a digital signature of B_{cast} formed with the private key of a voter casting the ballot

$DS(B_{\text{cast}}, v)$;

forming:

a digital signature of B_{cast} using a private key of the server $DS(B_{\text{cast}}, s)$,

associating B_{cast} , $DS(B_{\text{cast}}, v)$, and $DS(B_{\text{cast}}, s)$ with a vote serial number VSN;

forming a confirmation token, comprising:

$DS(B_{\text{cast}}, s)$, $DS(B_{\text{cast}}, v)$, VSN, and $DS(\text{Aggregation}, s)$,

where $DS(\text{Aggregation}, s)$ is the digital signature of the aggregation of the

associated B_{cast} , $DS(B_{\text{cast}}, v)$, $DS(B_{\text{cast}}, s)$, and VSN;

making the confirmation token available to a user;

receiving a confirmation token

extracting $VSN_{\text{received token}}$ and at least one of $DS_{\text{received token}}(B_{\text{cast}}, s)$, $DS_{\text{received token}}(B_{\text{cast}}, v)$,

and $DS_{\text{received token}}(AG, s)$ from the received token; and

for $VSN_{\text{received token}}$ and the corresponding VSN, comparing at least one of:

$DS_{\text{received token}}(B_{\text{cast}}, s)$ and $DS(B_{\text{cast}}, S)$;

$DS_{\text{received token}}(B_{\text{cast}}, v)$, and $DS(B_{\text{cast}}, v)$;

$DS_{\text{received token}}(\text{Aggregation}, s)$, and $DS(\text{Aggregation}, s)$;

if comparison shows equivalence between the data compared, determining that B_{cast} is verified.

32. (Previously Presented) The method of Claim 31 further comprising:

if comparison shows equivalence between $DS_{\text{received token}}(\text{Aggregation}, s)$, and

$DS(\text{Aggregation}, s)$, determining that the received confirmation token has not been modified since its formation.

33. (Previously Presented) A method for assisting a user verifying a cast ballot recorded in a server, the method comprising:

- receiving a cast ballot (" B_{cast} ") in a server;
- forming a digital signature of B_{cast} using a private key of the server (" $DS(B_{\text{cast}}, s)$ "),
- associating B_{cast} and $DS(B_{\text{cast}}, s)$ with a vote serial number (" VSN ");
- for VSN , comparing $DS(B_{\text{cast}}, s)$ and $DS(B_{\text{cast}}, S)$,
- if comparison shows equivalence between the data compared, determining that B_{cast} is verified.